УДК: 621.311 https://doi.org/10.15407/jai2024.02.020

О. І. Стасюк[1], Л. Л. Гончарова[2], Р. В. Грищук[3]
[1,2]Державний університет інфраструктури та технологій, Україна
9, вул. Кирилівська, м. Київ, 04071
[3]Житомирський військовий інститут імені С. П. Корольова, Україна
22, Проспект Миру, м. Житомир, 10004
[1]ostasuk177@gmail.com
[2]ktarae188@gmail.com
[3]Dr.Hry@i.ua
[1]https://orcid.org/0000-0002-2889-2288
[2]https://orcid.org/0000-0003-0116-0682
[3]https://orcid.org/0000-0001-9985-8477

МАТЕМАТИЧНІ МОДЕЛІ ВИЗНАЧЕННЯ ОПТИМАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ДИСТАНЦІЙ ЕЛЕКТРОПОСТАЧАННЯ ЗАЛІЗНИЦЬ

Анотація. Проведено дослідження проблеми безпеки інформаційних ресурсів інтелектуальних комп'ютерних мереж керування електропостачання в залізничній електроенергетиці. Представлено логічну структуру інтелектуальної комп'ютерної мережі, що відображає топологічні характеристики дистанції електропостачання, у вигляді графа. Запропоновано концептуальний підхід організації оптимальної стратегії кібербезпеки. На основі диференціальних перетворень Пухова запропоновано диференціальні математичні моделі для визначення в аналітичній формі ймовірностей стану вузлів графа. На основі принципу мінімаксу розроблено методи визначення оптимальної стратегії кібербезпеки, що дозволяє досягти заданих показників захищеності. Сформульовано критерій забезпечення безпеки інформації, що дозволяє визначити стан кібербезпеки кожного вузла графа та ймовірність перебування цього вузла в даному стані.

Ключові слова: кібербезпека, інтелектуалізація, кіберзагрози, математичні моделі, диференційні перетворення, інтелектуальні методи, вузол, граф, захист інформації, оптимальна стратегія, критерій.

O. Stasiuk[1], L. Goncharova[2], R. Hryshchuk[3]
[1,2] State University of Infrastructure and Technologies, Ukraine
9, st. Kyrylivska, Kyiv, 04071
[3] Korolyov Zhytomyr Military Institute, Ukraine
22, Prospect Myru, Zhytomyr, 10004
[1]ostasuk177@gmail.com
[2]ktarae188@gmail.com
[3]Dr.Hry@i.ua
[1]https://orcid.org/0000-0002-2889-2288
[2]https://orcid.org/0000-0003-0116-0682
[3]https://orcid.org/0000-0001-9985-8477

MATHEMATICAL MODELS FOR DETERMINING THE OPTIMUM CYBER SECURITY STRATEGY OF INTELLIGENT COMPUTER NETWORKS OF RAILWAY ELECTRICAL SUPPLY DISTANCES

Abstract. A study of the problem of the security of information resources of intelligent computer networks for power supply management in railway power generation was conducted. The logical structure of an intelligent computer network is presented, reflecting the topological characteristics of the power supply distance, in the form of a graph. A conceptual approach to the organization of an optimal cyber security strategy is proposed. On the based of Pukhov's differential transformations, differential mathematical models are proposed for determining, in analytical form, the state probabilities of graph nodes. Based on the minimax principle, methods have been developed to determine the optimal cyber security strategy, which allows to achieve the specified security indicators. A criterion for ensuring information security is formulated, which allows determining the state of cyber security of each graph node and the probability of this node being in this state.

Keywords: cyber security, intellectualization, cyber threats, mathematical models, differential transformations, intellectual methods, node, graph, information protection, optimal strategy, criterion.

Вступ

Сучасні залізничні системи, зокрема ті, що відповідають за дистанційне електропостачання, стають все більш інтелектуальними та інтегрованими. Відповідно, збільшується кількість потенційних точок входу для кіберзагроз, що можуть призвести до збоїв в електропостачанні, переривання залізничного руху та інших катастрофічних наслідків. Інтелектуальні комп'ютерні мережі залізниць значно залежать від інформаційних технологій для управління, моніторингу та оптимізації процесів електропостачання. Будь-які вразливості в цих системах можуть бути використані для кібератак, що може призвести до значних економічних збитків і загрози життю людей. Досвід експлуатації залізничних енергосистем показав, що невід'ємною частиною їх ефективного функціонування являється організація надійного захисту інформаційних ресурсів розподілених комп'ютерних мереж керування електроспоживанням [1-5]. Дослідження еволюції інноваційно - інвестиційного перетворення систем електропостачання залізничного транспорту і перспективних напрямків створення енергозберігаючих технологій електроспоживання на тягу, включаючи організацію безаварійних перевезень, сприяли появі і розвитку інтелектуальних комп'ютерних мереж керування електроспоживанням [3-6]. Організація інтелектуальних комп'ютерних мереж керування електропостачанням реалізується шляхом формування загальносистемної інформаційної моделі на принципах єдиного інформаційного простору і синхронної інформаційної взаємодії всіх компонентів, базуючись на взаємоінтеграції електромережевої топології і архітектури розподіленої комп'ютерної мережі. Синтезовані, таким чином, сучасні інтелектуальні комп'ютерні мережі орієнтовані, в першу чергу, на формування нових знань про об'єкт керування для оптимізації процесів оперативного і стратегічного управління електроспоживанням та створення новітніх енергозберігаючих і безаварійних технологій швидкісних перевезень. Використання сучасних інформаційних технологій в залізничній електроенергетиці створило передумови для розробки нових математичних моделей і методів кіберзахисту інформаційних ресурсів розподілених комп'ютерних мереж управління енергосистемою. Головним в процесі формування комплексу засобів захисту є організація відповідних стратегій безпеки для забезпечення цілісності інформаційних даних, фізичного збереження програмних ресурсів, нейтралізації випадкових або цілеспрямованих кибератак, ідентифікації можливих порушників і доступ до інформації, за умови відповідності ідентифікаторів визначеним [7]. Необхідний рівень захищеності комп'ютерної інформації може бути досягнутий шляхом організації сукупності спеціальних підсистем, інтегрованих в розподілену комп'ютерну мережу керування енергетикою, які в реальному часі електропостачання реалізують періодичний і епізодичний контроль, а також оцінку надійності функціонування системи в процесі реєстрації інформації, передачі, переробки і формуванні керуючих впливів.

Таким чином, актуальність оптимальної стратегії кібербезпеки інтелектуальних комп'ютерних мереж дистанцій електропостачання залізниць обумовлена необхідністю захисту критичної інфраструктури від постійно зростаючих та еволюціонуючих кіберзагроз, що мають суттєвий вплив на економічну стабільність, національну безпеку та безпеку населення.

Постановка задачі

Інтелектуальні комп'ютерні мережі можуть бути атаковані шкідливими програмами, які можуть знищити або викрасти важливу інформацію, порушити роботу систем або спричинити збій у постачанні електроенергії. Вирішенням проблеми кібернетичної і інформаційної

безпеки інтелектуальних комп'ютерних мереж керування електропостачанням дистанції залізниць тісно пов'язано з організацією швидкісних безаварійних перевезень і створенням нових енергозберігаючих технологій електропостачання. В основі ідеології організації інтелектуальних комп'ютерних мереж керування електропостачання закладено принцип адекватності топології дистанції електропостачання і архітектури розподіленого комп'ютерного середовища. Такий підхід дозволяє достатньо ефективно розв'язувати комплекс взаємообумовлених задач кібербезпеки інформаційних ресурсів, а також забезпечити цілісність, доступність і конфіденційність інформації в процесі виконання сукупності процедур управління швидкоплинними технологічними процесами електроспоживання [4-7]. Необхідно відмітити, що невід'ємною частиною систем кіберзахисту є здатність оцінювати на основі нових математичних моделей і методів підвищеної інтелектуальної складності і розмірності рівень ефективності програмно-апаратних засобів захисту інформаційних ресурсів, використовуючи критерії, що дозволяють враховувати сукупність особливостей технічних характеристик енергетичного об'єкта і архітектурних особливостей комп'ютерної мережі. Різноманітні компоненти та системи, які використовуються в інтелектуальних мережах, можуть мати різні рівні безпеки та бути не повністю сумісними одна з одною, що створює додаткові вразливості. Нагальна потреба в створенні оптимальної стратегії кібербезпеки стимулювала появу широкого спектру наукових досліджень в області створення нових концептуальних підходів і розробок математичних моделей і інтелектуальних методів моделювання кибератак на інформаційні ресурси. Сучасні критерії оцінки ефективності засобів захисту відкрила новий етап в області синтезу математичних моделей, комп'ютерно-орієнтованих методів і алгоритмів забезпечення безпеки підвищеної стійкості.

Мета роботи

Метою роботи є розробка математичних моделей і методів підвищеної інтелектуальної складності і розмірності організації оптимальної стратегії кібербезпеки інтелектуальних комп'ютерних мереж дистанцій електропостачання і критеріїв оцінки кібербезпеки інформаційних ресурсів.

Диференційні математичні моделі підвищеної інтелектуальної складності

Інтелектуальна розподілена комп'ютерна мережа дистанції електропостачання реалізує сукупність процедур управління швидкоплинними технологічними процесами постачання електричної енергії на тягу шляхом проведення безперервного ковзкого моніторингу штатних і аномальних режимів системи електропостачання, силового електроустаткування і систем релейного і мікропроцесорного захисту. Логічна структура розподіленої комп'ютерної мережі інтелектуальної системи дистанції електропостачання, що відображає її топологічні характеристики, може бути представлена у вигляді графа, як показано на рис. 1. Вузли графа представляють комп'ютерні засоби, які функціонально-орієнтовані на виконання тих або інших функцій ($P_0(t)$ - вузол, що представляє собою центральний сервер управління на рівні дистанції електропостачання; $P_1(t)$ - вузол сервера бази даних і формування єдиного інформаційного простору; $P_2(t)$ - центральний вузол зв'язку; $P_3(t)$ - вузол зв'язку з Internet; $P_4(t)$ - вузол сервера оперативного диспетчерського управління електропостачанням; $P_5(t)$ - вузол, що є сервером проведення моніторингу в залізничній енергетиці; $P_6(t)$ - вузол формування звітних документів; $P_7(t)$ - вузол інтелектуальної обробки і захисту інформації; $P_8(t)$ - вузол формування нових знань; $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ - вузли зв'язку з відповідними локальними

обчислювальними мережами тягових підстанцій) [4, 5].

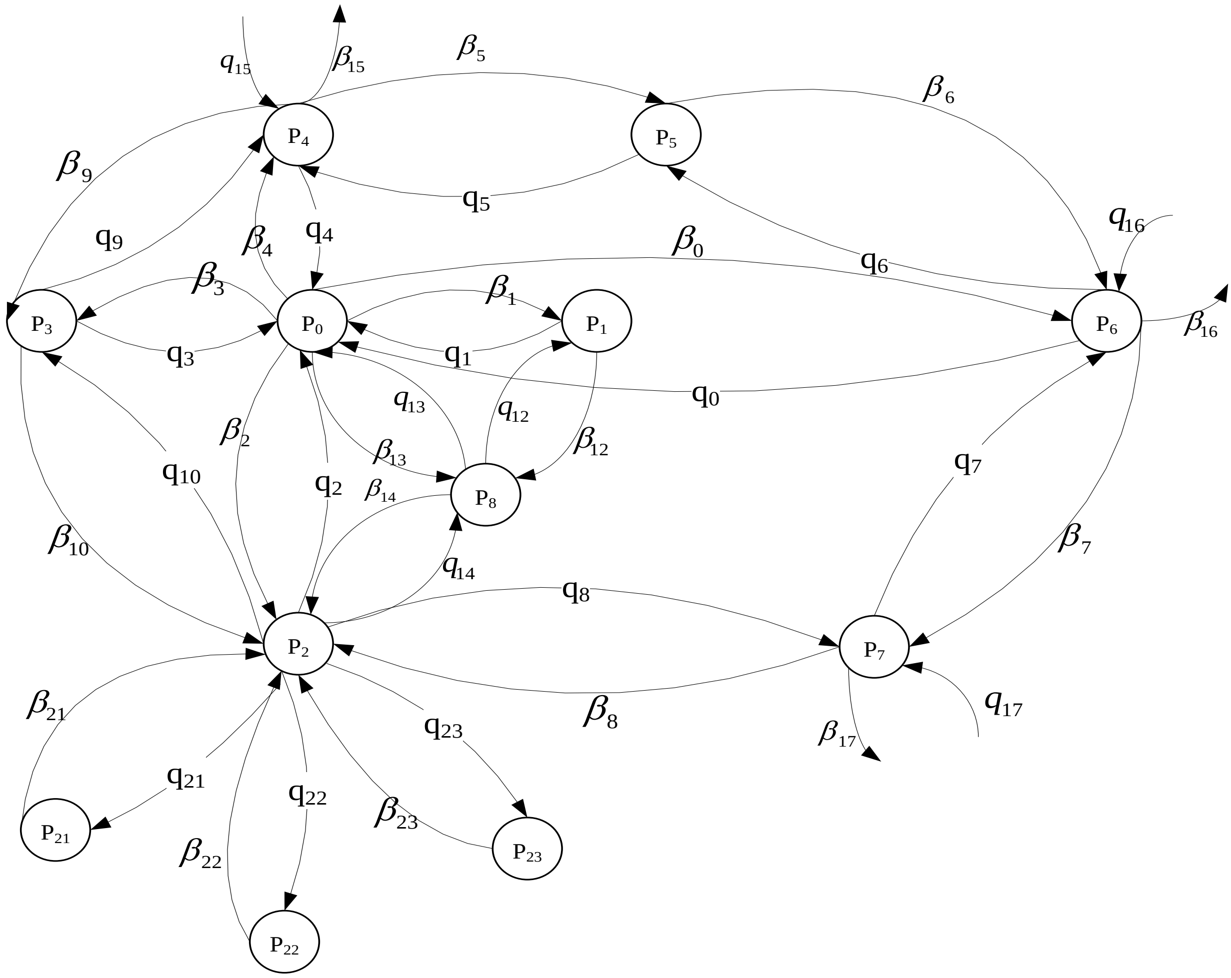


Рис. 1. Граф комп'ютерної мережі дистанції електропостачання залізниці

Інтенсивність потоку атак представлена величиною $q_i(t)$, а інтенсивність потоку захисних дій у відповідності як $\beta_i(t)$. Сукупність потоків, що протікають в системі, є основою переходу її з одного стану в інший.

Дослідження архітектури розподіленої комп'ютерної мережі всережимної системи керування електропостачанням дистанції залізниці, представленої у вигляді графа (рис. 1), будемо шляхом організації математичної моделі для визначення, в першу чергу, значень вірогідності $P_0(t),\ P_1(t),\ P_2(t),\ P_3(t),\ P_4(t),\ P_5(t),\ P_6(t), P_7(t), P_8(t),\ P_{21}(t),\ P_{22}(t),\ P_{23}(t)$ стану вузлів. З цією метою напишемо систему рівнянь Колмогорова, використовуючи для цього необхідний набір правил і формул [4-6]. Система диференціальних рівнянь для графу дистанції електропостачання залізниці (рис. 1), матиме вигляд

$$\begin{cases}
\frac{dP_0(t)}{dt} = -(\beta_1+\beta_2+\beta_3+\beta_4+\beta_0+\beta_{13})P_0(t)+q_0P_6(t)+q_1P_1(t)+q_4P_4(t)+q_3P_3(t)+q_2P_2(t)+q_{13}P_8(t);\\
\frac{dP_1(t)}{dt} = -(\beta_{12}+q_1)P_1(t)+\beta_1P_0(t)+q_{12}P_8(t);\\
\frac{dP_2(t)}{dt} = -(q_2+q_{14}+q_8+q_{23}+q_{22}+q_{21}+q_{10})P_2(t)+\beta_2P_0(t)+\beta_{14}P_8(t)+\beta_8P_7(t)+\beta_{23}P_{23}(t)+\beta_{22}P_{22}(t)+\beta_{21}P_{21}(t)+\beta_{10}P_3(t);\\
\frac{dP_3(t)}{dt} = -(q_9+q_3+\beta_{10})P_3(t)+\beta_9P_4(t)+\beta_3P_0(t)+q_{10}P_2(t);\\
\frac{dP_4(t)}{dt} = -(\beta_{15}+\beta_5+q_4+\beta_9)P_4(t)+q_5P_5(t)+\beta_4P_0(t)+q_9P_3(t);\\
\frac{dP_5(t)}{dt} = -(\beta_6+q_5)P_5(t)+\beta_5P_4(t)+q_6P_6(t);\\
\frac{dP_6(t)}{dt} = -(\beta_{16}+\beta_7+q_0+q_6)P_6(t)+q_7P_7(t)+\beta_0P_0(t)+\beta_6P_5(t);\\
\frac{dP_7(t)}{dt} = -(q_7+\beta_{17}+\beta_8)P_7(t)+\beta_7P_6(t)+q_8P_2(t);\\
\frac{dP_8(t)}{dt} = -(q_{12}+\beta_{14}+q_{13})P_8(t)+\beta_{12}P_1(t)+q_{14}P_2(t)+\beta_{13}P_0(t);\\
\frac{dP_{21}(t)}{dt} = -\beta_{21}P_{21}(t)+q_{21}P_2(t);\\
\frac{dP_{22}(t)}{dt} = -\beta_{22}P_{22}(t)+q_{22}P_2(t);\\
\frac{dP_{23}(t)}{dt} = -\beta_{23}P_{23}(t)+q_{23}P_2(t).
\end{cases} \quad (1)$$

З відповідними умовами $P_0(t)+P_1(t)+...+P_{23}(t)=1$ і початковими умовами $P_0(t_0)=1,\ P_1(t_0)=P_2(t_0)=\ldots=P_{23}(t_0)=0.$

З метою одержання узагальненого розв'язку системи диференціальних рівнянь (1) приймемо такі припущення

$$\beta=\beta_1=\beta_2=...=\beta_{23}, \text{ де } \beta_{\min}\le\beta\le\beta_{\max}, \quad (2)$$
$$q=q_1=q_2=...=q_{23}, \text{ де } q_{\min}\le q\le q_{\max}.$$

Тоді з урахуванням (2) математична модель (1) набуватиме вигляду

$$\begin{cases}
\frac{dP_0(t)}{dt} = -6\beta P_0(t)+q(P_6(t)+P_1(t)+P_4(t)+P_3(t)+P_2(t)+P_8(t));\\
\frac{dP_1(t)}{dt} = -(\beta+q)P_1(t)+\beta P_0(t)+qP_8(t);\\
.\\
.\\
.\\
\frac{dP_{23}(t)}{dt} = -\beta P_{23}(t)+qP_2(t).
\end{cases} \quad (3)$$

$$P_0(t_0)=1, P_1(t_0)=P_2(t_0)=...=P_{23}(t_0)=0.$$

Використовуючи положення теорії диференціальних перетворень, представимо систему рівнянь (3) в області зображень у вигляді диференціальної математичної моделі. Для цього застосуємо диференціальні перетворення Пухова, представлені наступною парою математичних залежностей [4-8].

$$P(k) = \frac{H^k}{k!}\left[\frac{d^k p(t)}{dt^k}\right] \doteq \; p(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P(k), \qquad (4)$$

де $p(t)$ - оригінал, що являє собою безперервну функцію дійсного аргументу t, що диференціюється нескінченну кількість разів і обмежену разом із всіма своїми похідними; $P(k)$ - диференціальне зображення оригіналу $p(t)$, що є дискретною функцією цілочислового аргументу $k = 0, 1, 2, \ldots$; H – масштабна стала, яка має розмірність аргументу t і часто обирається такою, що дорівнює відрізку $0 \leq t \leq H$, на якому розглядається функція $p(t)$; $\doteq$ - символ відповідності між оригіналом $p(t)$ і його диференційним зображенням $P(k)$. У перетвореннях (4) зліва від символу $\doteq$ стоїть пряме перетворення, що дозволяє за оригіналом $p(t)$ знайти зображення $P(k)$, а праворуч – обернене, що дозволяє за зображенням $P(k)$ отримати оригінал $p(t)$ у формі степеневого ряду, який є рядом Тейлора з центром у точці $t = 0$. У подальшому зображення $P(k)$ називатимемо диференційними спектрами, а при конкретних значеннях k – дискетами.

Скориставшись прямим перетворенням (4), сформуємо диференційну математичну модель, що представляє собою систему диференціальних рівнянь (5), представлену в області зображень з початковими умовами, які в області диференційних зображень можуть бути представлені наступним чином

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}(-6\beta P_0(k) + q(P_6(k) + P_1(k) + P_4(k) + P_3(k) + P_2(k) + P_8(k))); \\ P_1(k+1) = \dfrac{T}{k+1}(-(\beta + q)P_1(k) + \beta P_0(k) + qP_8(k)); \\ . \\ . \\ . \\ P_{23}(k+1) = \dfrac{T}{k+1}(-\beta P_{23}(k) + qP_2(k)). \end{cases} \qquad (5)$$

$$P_0(t) = P_0(0) = 1,\; P_i(t) = P_i(0) = 0,\; P_{2i}(t) = P_{2i}(0) = 0, k = 0,\; t_0 = 0,\; i = 0,1,2\ldots,$$

де T – тривалість процесу моделювання, що обрана рівною H, тобто $T = H$.

Отримана диференційна математична модель (5) є основою визначення, в аналітичному вигляді, значень ймовірностей

$$P_0(t),\; P_1(t)\; P_2(t),\; P_3(t)\; P_4(t),\; P_5(t),\; P_6(t),\; P_7(t),..\; P_{21}(t),\; P_{22}(t)\; P_{23}(t)$$

вузлів графа, що відображає комп’ютерну архітектуру системи управління дистанції електропостачання на тягу. Після підстановки початкових умов

$$P_0(t) = P_0(0) = 1,\; P_i(t) = P_i(0) = 0,\; P_{2i}(t) = P_{2i}(0) = 0, k = 0,\; t_0 = 0,\; i = 0, 1, 2\;\ldots$$

в диференційну математичну модель (5) і виконавши ряд математичних процедур при $k=0$, $k=1$, $k=2$, … та використавши зворотне диференційне перетворення $p(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P(k)$ згідно (4), отримаємо значення $P_0(t)$, $P_1(t)$ $P_2(t)$, $P_3(t)$ $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$,.. $P_{21}(t)$, $P_{22}(t)$ $P_{23}(t)$ в аналітичному вигляді.

З метою спрощення аналізу, розглянемо процедуру обчислення сукупності дискрет $P_0(0)$, $P_0(1)$, $P_0(2)$ …, для визначення ймовірності $P_0(t)$ стану тільки першого вузла графа (рис. 1). Не важко переконатися, що при виконанні обчислювального процесу за допомогою диференційної математичної моделі (5) при $k=0$, $k=1$, $k=2$, … отримаємо

$$P_0(0)=[P_0(t_0)]=1;\ k:=0\rightarrow P_0(1)=-6\beta T;\ k:=1\rightarrow P_0(2)=3\beta T^2(6\beta+q); \qquad (6)$$

$$k:=2\rightarrow P_0(3)=-\frac{1}{3}\beta T^3(108\beta^2+\frac{75}{2}\beta q+6q^2)$$

Використавши зворотне диференційне перетворення $p(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P(k)$ згідно (4), напишемо, в аналітичному вигляді, значення $P_0(t)$ ймовірності першого вузла як

$$P_0=1-6\beta T+3\beta(q+6\beta)t^2-\frac{1}{3}\beta(108\beta^2+\frac{75}{2}\beta q+6q^2)t^3 \qquad (7)$$

Формування оптимальної стратегії кібербезпеки

Оскільки завдання безпеки інформаційних ресурсів в комп'ютерних мережах вирішуються в умовах антагонізму суб'єктів інформаційного конфлікту, то, незважаючи на це, домінуючим в таких умовах є дотримання суб'єктами конфлікту принципу мінімаксу. Досягнення системою заданих показників захищеності можливо шляхом раціонального визначення стратегії формування таких значень, які мінімізують плату суб'єкта забезпечення безпеки за витрачені відповідні ресурси при максимальній інтенсивності потоків кибератак.

Досягнення системою заданих показників захищеності можливо шляхом раціонального визначення стратегії формування таких значень $\beta_i(t)$, які мінімізують плату суб'єкта забезпечення безпеки $\theta_i(q_j,\beta_j)$ за витрачені відповідні ресурси при максимальній інтенсивності потоків кибератак $q_i(t)$, тобто

$$\theta_i^*(q_j,\beta_j)=\min_{\beta_j\in E_\beta}\max_{q_j\in E_q}\theta_i(q_j,\beta_j),\ i=0,1,2,\dots\ j=0,1,2,\dots \qquad (8)$$

В процесі моделювання стратегії кибератак, протиборчі сторони ймовірно виходять з умови формування таких стратегій $q_i(t)$, які максимізували плату $\beta_i(t)$, за умови її мінімізації системою кібербезпеки, тобто

$$\theta_i^*(q_j,\beta_j)=\min_{q_j\in E_q}\max_{\beta_j\in E_\beta}\theta_i(q_j,\beta_j),\ i=0,1,2\dots,\ j=0,1,2\dots \qquad (9)$$

Очевидно, що при умові виконання математичних залежностей (8), (9)

$$\min_{\beta_j\in E_\beta}\max_{q_j\in E_q}\theta_i(q_j,\beta_j)=\max_{q_j\in E_q}\min_{\beta_j\in E_\beta}\theta_i(q_j,\beta_j)=\theta_i^{*opt}(q_j^{opt},\beta_j^{opt}), \qquad (10)$$

пошукові стратегії $q_i(t)^{\text{opt}}$ і $\beta_i(t)^{\text{opt}}$, називаються оптимальними. Стратегія забезпечення безпеки інформації полягає в пошуку закону зміни потоку інтенсивності захисних дій $\beta_i(t)$, яка реалізує мінімізацію функціонала (8) при стохастичній інтенсивності потоків кибератак $q_i(t)$ у відповідних межах. Тому, у зв'язку з антагонізмом цілей суб'єктів інформаційного конфлікту, домінуючою стратегією забезпечення безпеки інформації буде стратегія на основі принципу мінімаксу [7, 8], тобто

$$\min_{\beta_j \in E_\beta} \max_{q_j \in E_q} \theta_i\left(t, P_i q_j, \beta_j\right). \qquad (11)$$

Застосування мінімаксної стратегії (11) дозволяє мінімізувати функціонал (8) навіть у випадках найгіршого поєднання інтенсивності потоків кибератак $q_i(t)$ з довільним законом потоку інтенсивності по захисних діях $\beta_i(t)$.

Критерії кібербезпеки

Використавши значення ймовірностей $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$, $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$, ... $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ вузлів графа локальної мережі управління дистанції електропостачанням, обчислених по аналогії з (6, 7), можна написати критерій захищеності інформаційних ресурсів у вигляді [4-6]

$$\theta_i(t) = \frac{1}{T}\int_{t=t_0}^{T} P_i(t)dt, \; i = 0,1,2\ldots \, . \qquad (12)$$

Згідно (12), стан кібербезпеки P_0- го вузла для графу дистанції електропостачання залізниці визначається виразом

$$\theta_0(t) = \frac{1}{T}\int_{t_0}^{T} P_0(t)dt \, .$$

Скориставшись прямим диференційним перетворенням (4), критерій

$$\theta_0(t) = \frac{1}{T}\int_{t_0}^{T} P_0(t)dt$$

набуває вигляду

$$\theta_0 = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1} \qquad (13)$$

Після підстановки сукупності дискрет (6) в (13) модель стану кібербезпеки P_0- го вузла для $k = 0,1,2,\ldots$ набуватиме вигляду

$$\theta_0 = 1 - 3\beta T + \beta T^2 (6\beta + q) - \frac{1}{12}\beta T^3 (108\beta^2 + \frac{75}{2}\beta q + 6q^2) \, . \qquad (14)$$

Дослідження функціоналу (14) на екстремум дозволяє в загальному вигляді визначити оптимальні стратегії $q_i(t)^{\text{opt}}$ і $\beta_i(t)^{\text{opt}}$ розподілу ресурсів, що витрачаються на захист і, відповідно на кібератаку P_0- го вузла

$$\begin{cases} \dfrac{\partial \theta_0(\beta, q)}{\partial \beta} = 0; \\ \dfrac{\partial \theta_0(\beta, q)}{\partial q} = 0. \end{cases} \qquad (15)$$

Як наслідок з (15), маємо

$$\begin{cases} \beta^{opt} = \dfrac{16}{71T} \\ q^{opt} = \dfrac{21}{71T} \end{cases} \qquad (16)$$

Дослідження (13) на достатні умови дозволяє визначити спосіб визначення екстремуму знайдених стратегій (16), тобто

$$\begin{cases} \dfrac{\partial^2 \theta_0(\beta^{opt}, q^{opt})}{\partial^2 \beta^{opt}} > 0; \\ \dfrac{\partial^2 \theta_0(\beta^{opt}, q^{opt})}{\partial^2 q^{opt}} < 0. \end{cases} \qquad (17)$$

Після відповідних перетворень, на основі (14), (17) другі похідні приймають наступні значення

$$\begin{cases} \dfrac{\partial^2 \theta_0(\beta^{opt}, q^{opt})}{\partial^2 \beta^{opt}} = 12T^2; \\ \dfrac{\partial^2 \theta_0(\beta^{opt}, q^{opt})}{\partial^2 q^{opt}} = -\beta T^3. \end{cases} \qquad (18)$$

Вираз (18) показує, що достатні умови (17) виконуються. Отже, знайдені в (16) інтенсивності $q_i(t)^{\text{opt}}$ і $\beta_i(t)^{\text{opt}}$ є відповідно мінімумом та максимумом, тобто

$$\begin{cases} \beta^{opt} = \beta^{opt}_{\min}; \\ q^{opt} = q^{opt}_{\max}. \end{cases} \qquad (19)$$

Стан кібербезпеки P_0 - го вузла згідно виразу (19) і відповідно (13) дорівнюватиме

$$\theta_0 = 0{,}54 \qquad (20)$$

Ймовірність перебування P_0 - го вузла в захищеному стані, згідно (7), при виборі оптимальних значень інтенсивності $q_i(t)^{\text{opt}}$ і $\beta_i(t)^{\text{opt}}$, по виразам (15-19) може бути описана моделлю у вигляді

$$P_0^{opt}(t) = 1 - \frac{96}{71}\frac{t}{T} + \frac{5616}{5041}\left(\frac{t}{T}\right)^2 - \frac{228768}{357911}\left(\frac{t}{T}\right)^3. \qquad (21)$$

Отже, одержані аналітичні вирази (7) та (14) для P_0 - го вузла дистанції електропостачання залізниці дозволяють визначити стан кібербезпеки даного вузла відповідно (20) та ймовірність перебування цього вузла в даному стані відповідно математичній залежності (21).

Висновки

1. Дослідження проблеми безпеки інформаційних ресурсів інтелектуальних комп’ютерних мереж керування електропостачання в залізничній електроенергетиці показали, що для організації безаварійних швидкісних перевезень, створення перспективних енергозберігаючих технологій електроспоживання і формування нових знань в предметній області необхідно створити новий клас математичних моделей підвищеної інтелектуальної складності і розмірності та методів формування оптимальних стратегій кіберзахисту інформаційних ресурсів розподілених комп’ютерних мереж управління енергосистемою.

2. Для аналізу, з точки зору захисту інформації, логічну структуру інтелектуальної комп'ютерної мережі, що відображає топологічні характеристики дистанції електропостачання, представлено у вигляді графа, на основі якого запропоновано концептуальний підхід організації оптимальної стратегії кібербезпеки, методи моделювання кибератак на інформаційні ресурси і сучасні критерії оцінки ефективності засобів захисту підвищеної стійкості.

3. На основі фундаментальних положень теорії диференціальних перетворень Пухова запропоновано диференційні математичні моделі для визначення, в аналітичній формі, ймовірностей стану вузлів графа розподіленої обчислювальної мережі дистанції електропостачання, як основи створення інтелектуальних засобів захисту інформаційних ресурсів.

4. Запропоновано методи визначення оптимальної стратегії кібербезпеки інтелектуальних комп’ютерних мереж на основі приведених необхідних і достатніх умов існування екстремуму, що відкриває можливість на базі принципу мінімаксу досягти заданих показників захищеності шляхом формування закону зміни потоку інтенсивності захисних дій при стохастичній максимальній інтенсивності потоків кибератак.

5. Сформульовано в сфері диференційних зображень критерій забезпечення безпеки інформації і отримані

аналітичні вирази для кожного вузла інтелектуальної комп'ютерної мережі дистанції електропостачання залізниці, що дозволяють визначити стан кібербезпеки даного вузла та ймовірність перебування цього вузла в даному стані.

Література

1. Стратегія розвитку штучного інтелекту в Україні. За загальною редакцією А. І. Шевченка. Видавництво «Торпеда». Київ – 2023 р. С 306

2. Sopel, M., Stasyuk, O., Kuznetsov, V., Goncharova, L., Hubskyi, P. Regina computer system for intelligent monitoring, diagnostics, and management of railway power supply systems Diagnostykathis link is disabled, 2021, 22(4), стр. 77–88 (Scopus) (Q3). https://www.scopus.com/authid/detail.uri?authorId=57191292791

3. Stasiuk, A., Kuznetsov, V., Goncharova, L., Hubskyi, P. Models of the computer intellectualization optimal strategy of the power supply fast-flowing technological processes of the railways traction substations. Communications - Scientific Letters of the University of Zilina, 2021, 23(2), стр. C30–C36. (Scopus) (Q3). http://komunikacie.uniza.sk/index.php/communications/article/view/1680

4. Stasiuk O.I., Goncharova L.L. Mathematical Models and Methods for Analyzing Computer Control Networks of Railway Power Supply. New Means Cybernetics, Informatics, Computers Engineering and Systems Analysis. Springer Science+Business Media New York 2018. Volume 54, Issue 1, February 2018, Pages 165-172. (Scopus) (Q3). https://link.springer.com/article/10.1007/s10559-018-0017-0

5. Stasiuk A.I., Hryshchuk, R.V., Goncharova L.L. Mathematical differential models and methods for assessing the cybersecurity of computer networks intelligent control of technological processes of railway power supply. New Means Cybernetics, Informatics, Computers Engineering and Systems Analysis. Springer Science+Business Media New York 2018. Volume 54, Issue 4, February 2018, Pages 671-68. (Scopus) (Q3). https://link.springer.com/article/10.1007/s10559-018-0068-2

6. Stasiuk A.I., Hryshchuk, R. V., Goncharova L. L. A Mathematical Cybersecurity Model of a Computer Network for the Control of Power Supply of Traction Substations. Cybernetics and Systems Analysis. Springer Science+Business Media New York Volume 53, Issue 3, May 2017, Pages 476-484. https://link.springer.com/article/10.1007/s10559-017-9949-z https://www.scopus.com/authid/detail.uri?authorId=57191292791

7. Stasyuk, A.I., Lidiya L. Goncharova, Mathematical models and methods of the analysis of computer networks of control of power supply of railways traction substations L.L. Journal of Automation and Information Sciencesthis link is disabled, 2017, 49(2), стр. 50–60. https://www.dl.begellhouse.com/ru/journals/2b6239406278e43e,5bdc44c95254b2ed,779791cb12ca6912.html

8. Alexander I. Stasiuk, Lidiya L. Goncharova Mathematical Models and Methods of Formation of Intelligent Computer Networks for Control of Power Supply and Optimization of Power Consumption of Railways. Journal of Automation and Information Sciences. Begell House Inc. (США), New York, Connecticut. Volume 50, 2018 Issue 8 , pages 50-65. SCOPUS, Web of Science, ISI, INIS Atomindex, io-port.net. http://www.dl.begellhouse.com/journals/2b6239406278e43e,2ec3cf2b062398ac,5e87262e3b8eefd4.html

9. Pukhov G.E., Taylor transformations and their application in electrical engineering and electronics [in Russian], Naukova dumka, Kiev, 1978.

References

1. Stratehiia rozvytku shtuchnoho intelektu v Ukraini. Za zahalnoiu redaktsiieiu A. I. Shevchenka. Vydavnytstvo «Torpeda». Kyiv – 2023 r. S 306.

2. Sopel, M., Stasyuk, O., Kuznetsov, V., Goncharova, L., Hubskyi, P. Regina computer system for intelligent monitoring, diagnostics, and management of railway power supply systems Diagnostykathis link is disabled, 2021, 22(4), стр. 77–88 (Scopus) (Q3). https://www.scopus.com/authid/detail.uri?authorId=57191292791

3. Stasiuk, A., Kuznetsov, V., Goncharova, L., Hubskyi, P. Models of the computer intellectualization optimal strategy of the power supply fast-flowing technological processes of the railways traction substations. Communications - Scientific Letters of the University of Zilina, 2021, 23(2), стр. C30–C36. (Scopus) (Q3). http://komunikacie.uniza.sk/index.php/communications/article/view/1680

4. Stasiuk O.I., Goncharova L.L. Mathematical Models and Methods for Analyzing Computer Control Networks of Railway Power Supply. New Means Cybernetics, Informatics, Computers Engineering and Systems Analysis. Springer Science+Business Media New York 2018. Volume 54, Issue 1, February 2018, Pages 165-172. (Scopus) (Q3). https://link.springer.com/article/10.1007/s10559-018-0017-0

5. Stasiuk A.I., Hryshchuk, R.V., Goncharova L.L. Mathematical differential models and methods for assessing the cybersecurity of computer networks intelligent control of technological processes of railway power supply. New Means Cybernetics, Informatics, Computers Engineering and Systems Analysis. Springer Science+Business Media New York 2018. Volume 54, Issue 4, February 2018, Pages 671-68. (Scopus) (Q3). https://link.springer.com/article/10.1007/s10559-018-0068-2

6. Stasyuk, A.I., Lidiya L. Goncharova,

Mathematical models and methods of the analysis of computer networks of control of power supply of railways traction substations L.L. Journal of Automation and Information Sciencesthis link is disabled, 2017, 49(2), стр. 50–60.
https://www.dl.begellhouse.com/ru/journals/2b623940 6278e43e,5bdc44c95254b2ed,779791cb12ca6912.html

7. Alexander I. Stasiuk, Lidiya L. Goncharova Mathematical Models and Methods of Formation of Intelligent Computer Networks for Control of Power Supply and Optimization of Power Consumption of Railways. Journal of Automation and Information Sciences. Begell House Inc. (США), New York, Connecticut. Volume 50, 2018 Issue 8 , pages 50-65. SCOPUS, Web of Science, ISI, INIS Atomindex, io-port.net.
http://www.dl.begellhouse.com/journals/2b623940627 8e43e,2ec3cf2b062398ac,5e87262e3b8eefd4.html

8. Pukhov G.E., Taylor transformations and their application in electrical engineering and electronics [in Russian], Naukova dumka, Kiev, 1978.

The article has been sent to the editors 15.06.24.
After processing 20.06.24.
Submitted for printing 28.06.24.

.